CS 70 Discrete Mathematics and Probability Theory
Fall 2017 Satish Rao and Kannan Ramchandran

HW 4

Sundry

Before you start your homework, write down your team. Who else did you work with on this homework? List names and email addresses. (In case of homework party, you can also just describe the group.) How did you work on this homework? Working in groups of 3-5 will earn credit for your "Sundry" grade.

Please copy the following statement and sign next to it:

I certify that all solutions are entirely in my words and that I have not looked at another student's solutions. I have credited all external sources in this write up.

1 Don't Try This at Home

A ticket in the lottery consists of six numbers chosen from $1,2,\ldots,48$ (repetitions allowed). After everyone has bought their tickets, the manager picks 5 winning numbers from this set at random. Your ticket wins if it contains each of these winning numbers. Order is irrelevant.

Prove that if you buy all possible tickets for which the sum of the six entries on the ticket is divisible by 47, then you are guaranteed to have a winner.

2 Euclid's Algorithm

(a) Use Euclid's algorithm from lecture to compute the greatest common divisor of 527 and 323. List the values of x and y of all recursive calls.

(b) Use extended Euclid's algorithm from lecture to compute the multiplicative inverse of 5 mod 27. List the values of x and y and the returned values of all recursive calls.

(c) Find $x \pmod{27}$ if $5x+26 \equiv 3 \pmod{27}$. You can use the result computed in (b).

(d) Assume a, b, and c are integers and $c > 0$. Prove or disprove: If a has no multiplicative inverse mod c, then $ax \equiv b \pmod{c}$ has no solution.

3 Solution for $ax \equiv b \pmod{m}$

In the notes, we proved that when $\gcd(m,a) = 1$, a has a unique multiplicative inverse, or equivalently $ax \equiv 1 \pmod{m}$ has exactly one solution x (modulo m). This proof also implies that when $\gcd(m,a) = 1$, there is a unique solution to $ax \equiv b \pmod{m}$, where x is the unknown variable.

Now consider the equation $ax \equiv b \pmod{m}$, when $\gcd(m,a) > 1$.

(a) Let $\gcd(m,a) = d$. Prove that $ax \equiv b \pmod{m}$ has a solution (that is, there exists an x that satisfies this equation) if and only if $b \equiv 0 \pmod{d}$.

(b) Let $\gcd(m,a) = d$. Assume $b \equiv 0 \pmod{d}$. Prove that $ax \equiv b \pmod{m}$ has exactly d solutions (modulo m).

(c) Solve for x: $77x \equiv 35 \pmod{42}$.

4 Nontrivial Modular Solutions

(a) What are all the possible squares modulo 4? Show that any solution to $a^2 + b^2 \equiv 3c^2 \pmod{4}$ must satisfy $a^2 \equiv b^2 \equiv c^2 \equiv 0 \pmod{4}$.

(b) Using part (a), prove that $a^2 + b^2 = 3c^2$ has no non-trivial solutions (a,b,c) in the integers. In other words, there are no integers a, b, and c that satisfy this equation, except the trivial solution $a = b = c = 0$.

[*Hint:* Consider some nontrivial solution (a,b,c) with the smallest positive value for a (why are we allowed to consider this?). Then arrive at a contradiction by finding another solution (a',b',c') with $a' < a$.]